STATEWIDE INFORMATION SYSTEMS POLICY

Statewide Policy: Workstation, Portable Computer, and PDA (Personal Digital Assistant) Security

Product ID: ENT-SEC-112

Effective Date: October 2004

Approved: Steve Bender, Acting Director, Department of Administration

Replaces & Supercedes: This policy supercedes any prior enterprise policies for establishing and implementing information technology (IT) policies and standards.

I. Authorizations, Roles, & Responsibilities

Pursuant to the Montana Information Technology Act ("MITA") (Title 2, Chapter 17, Part 5 of the Montana Code Annotated ("MCA"), it is the policy of the state that information technology be used to improve the quality of life of Montana citizens, and that such improvement is to be realized by protecting individual privacy and the privacy of the information contained within the state's information technology systems. §2-17-505(1), MCA. It is also the policy of the state that the development of information technology resources be conducted in an organized, deliberative, and cost-effective manner, which necessitates the development of statewide information technology policies, standards, procedures, and guidelines applicable to all state agencies and others using the state network. It is also anticipated that State information technology systems will be developed in cooperation with the federal government and local governments with the objective of providing seamless access to information and services to the greatest degree possible. §2-17-505(2), MCA.

Department of Administration: Under MITA, the Department of Administration ("DOA") is responsible for carrying out the planning and program responsibilities for information technology for state government (except the national guard), including for establishing and enforcing a state strategic information technology plan and establishing and enforcing statewide information technology policies and standards. DOA is responsible for implementing MITA and all other laws for the use of information technology in state government. The director of DOA has appointed the chief information officer to assist in carrying out the department's information technology duties. §2-17-512, MCA.

Department Heads: Each department head is responsible for ensuring an adequate level of security for all data within their department. §2-15-114, MCA.

II. Policy - Requirements

A. Scope

This policy applies to all computers that are owned by the state and/or are connected to state resources. This policy does not apply to colleges and universities, the Commissioner of Higher Education Office, or public access computers in libraries.

B. Purpose

This policy is intended to establish minimum standards for the security of workstations, portable computers and PDA's owned by the State of Montana.

C. Definitions

Portable - for the purposes of this policy, a portable computer includes a laptop, pocket PC, tablet, or notebook, portable computers (such as Personal Digital Assistants [PDAs], smart phones, etc.), and any other computers being used to connect to the state's network remotely.

D. Requirements

Computer users are responsible for maintaining the physical security of their own workstation, portable computer, and/or PDA and for following the security requirements implemented by the Department of Administration and by the agency at which they are employed. Workstations, portable computers, and PDA's should be kept out of sight and covered when stored in a vehicle.

Any software installed on workstations, portable computers or PDA's that uses script files must not contain a userID or password for the state's computer system.

Workstations with unattended processes running on them must have some type of screen saver with password protection or keyboard locking program enabled on them.

Portable computers MUST be transported as carry-on luggage when traveling by plane or bus, unless the carrier requires otherwise.

All workstations, portable computers, and PDA's must be updated with the latest security patches, virus scanning software and virus data files. Agencies are responsible for installing the patches, virus scanning software and virus data files on their devices. Patches and updates to virus data files should be installed through an automated process if applicable. Agencies are required to install patches for high-risk vulnerabilities within 48 hours of notification.

Firewall software must be installed, updated, and used according to standards set by ITSD on all portable computers used to connect outside of the state (Internet) firewall.

All PDA's used to connect directly to state computers must be state owned.

Policy changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this policy are made by submitting an Action Request form. Requests for exceptions are made by submitting an Exception Request form.

E. Background - History On The Creation Of Or Changes To This Policy

This policy was originally created by the NetWare Managers Group Policy Committee. This policy was updated by the Security Section of ITSD in January 2002 and reviewed with the Information Technology Managers Council prior to adoption.

F. Guidelines - Recommendations, Not Requirements

If highly sensitive or confidential information is stored on a portable computer or PDA, the data should be encrypted.

In accordance with ENT-SEC-071, the following information should appear on portable computers when powered on: "This computer is the property of the State of Montana, Department of <department name> and subject to the appropriate use policies located at: http://itsd.mt.gov/policy/itpolicy.asp. Unauthorized use is a violation of 45-6-311, MCA."

Power on or system passwords should be used on workstations that are in highly accessible areas and on portable computers. Power on passwords should be provided to the Network Administrator and kept in a secure place.

Patches and updates should be completed with an automated process if applicable.

G. Change Control and Exceptions

Policy changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this policy are made by submitting an Action Request form. Requests for exceptions are made by submitting an Exception Request form. Changes to policies and standards will be prioritized and acted upon based on impact and need.

III. Close

For questions or comments about this instrument, contact the Information Technology Services Division at ITSD Service Desk, or:

Chief Information Officer
PO Box 200113
Helena, MT 59620-0113
(406) 444-2700
FAX: (406) 444-2701

IV. Cross-Reference Guide

A. State/Federal Laws

- 2-17-505(1) – Policy
- 2-17-514(1) – Enforcement
- §2-17-505(2), MCA
- §2-17-512, MCA
- §2-15-114, MCA
- 2-17-534, MCA
- 45-6-311, MCA

B. State Policies (IT Policies, MOM Policies, ARM Policies)

- 2-15-112, MCA
- 1-0250.00, MOM
- ARM 2.13.101 - 2.13.107 - Regulation of Communication Facilities
- MOM 3-0130 Discipline
- ARM 2.12.206 Establishing Policies, Standards, Procedures and Guidelines.

C. IT Procedures or Guidelines Supporting this Policy

- Policy: Establishing and Implementing Statewide Information Technology Policies and Standards
- Procedure: Establishing and Implementing Statewide Information Technology Policies and Standards

V. Administrative Use

Product ID:	ENT-SEC-112
Proponent:	Steve Bender, Acting Director, Department of Administration
Version:	1.1
Approved Date:	July 15, 2008
Effective Date:	October 2004
Change & Review Contact:	ITSD Service Desk
Review Criteria:	Event Review: Any event affecting this policy may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date:	July 1, 2013
Last Review/Revision:	Reviewed July 11, 2008. Non-material changes are necessary.
Change Record:	July 11, 2008 – Non-material changes made: - Standardize instrument format and common components. - Changed to reflect next review date.